REMARKS

Reconsideration and allowance of the claims pending in the application are requested

Claims 1-28 are pending in the application. The pending claims have been rejected in the subject Office Action, dated February 28, 2006, as follows:

Claim 28 has been rejected under 35 USC 112, second paragraph as an omnibus claim and indefinite.

Claims 25-27 have rejected under 35 USC 112, second paragraph as indefinite based on insufficient antecedents.

Claim 25 has been objected to based on informality.

Claims 1-7, 12-15, 17 and 23-28 have been rejected under 35 USC 102 (e) as anticipated by USP 6,944,765 B1 to G. G. Rose, et al issued September 13, 2005 and filed December 21, 19999 (Rose).

Claims 8, 9, and 11 have been rejected under 35 USC 103(a) as being unpatentable over Rose as applied to claim 5 above, and further in view of USP 6,549,210 B1 to Van Hook et al. (Van Hook), of record.

Claims 10 and 18 have been rejected under 35 USC 103(a) as being unpatentable over Rose as applied to claims 5 and 13 above and further in view of USP 6,662,167 B1 to Xiao, of record (Xiao).

Claims 16 and 19-21 have been rejected under 35 USC 103(a) as being unpatentable over Rose as applied to claim 13 above and further in view as applied to USP 5,768,385 to Simon, of record (Simon).

Claim 22 has been rejected under 35 USC 103(a) as being unpatentable over Rose as applied to claim 13 above and further in view of USP 6,233,291 to Puhl, of record.

The application has been amended to cure the rejections under 35 USC 112, second paragraph. The rejection of claims 1-28 has been traversed.

Before responding to the rejections, Applicants would like to distinguish the subject matter of claims 1- 28 from the Rose, as follows:

Rose discloses a method of preventing a person from impersonating a plurality of users of software. The method advantageously includes the steps of constructing a plurality of puzzles, each puzzle having a solution that includes information about a respective one of the plurality of users, each puzzle requiring consumption of a resource to solve; and sending each puzzle to a respective one of the plurality of users for solution.

Rose fails to disclose the claimed subject matter, as follows:

1. There is no distributed computational task being accomplished. The task is individual to the user. In fact, all claims state explicitly that the goal is to authenticate users of software, not to distribute a computational task among them. Rose fails to disclose distributing a computational task among a plurality of entities.

2. Rose discloses the user returns the puzzle to the provider at a later time, as described at column 3, lines 13 -15. In contrast, Jakobsson discloses a Prover demonstrates a certain amount of computation has been performed within a specified interval of time as described in Jakobsson at page 5, lines 10 -15. Rose fails to disclose an entity demonstrating a certain amount of computation has been performed within a specified interval of time.

3. Rose discloses the Provider receives the answer to a puzzle from a user, and not from one of a plurality of users because the puzzle includes user information, as described at column 3, lines 2-13. In contrast, Jakobsson discloses a first entity receives response from a second entity based on the response from several third entities, as described at page 3, lines 17-23. Rose fails to disclose a first entity receiving a response compiled from more than two entities.

4. Rose discloses a software distributor distributes software to a user solving a puzzle provided by the distributor. The puzzle is user specific, as described in Rose at column 2,

lines 27-32. In contrast, Jakobsson at page 4, lines 3-7 discloses a POW can be recycled to other entities as a bread pudding protocol. Rose fails to disclose recycling a puzzle of a user to another user.

Summarizing, Rose addresses an authentication problem by a user solving a user specific puzzle which is not recyclable by a provider. In contrast, Jakobsson discloses an entity or prover solving an authentication problem, via a plurality of entities in behalf of the prover demonstrating performance of a computational task within a specified time interval as a Proof of Work (POW). The POW is recyclable. Rose fails to disclose the claimed subject matter and does not support the rejection of claims 1-28 under 35 USC 102 (e) or 103 (a). Withdrawal of the rejection and allowance of claims 1 – 28 are requested.

Now turning to the rejection, Applicants respond to the indicated Paragraphs of the subject Office Action, as follows:

Paragraphs 1-6:

The Examiner's comments are noted. No response is believed necessary.

Paragraph 7:

Claim 28 has been amended to describe the term "efficient" as, wherein w is less than z the maximum amount of computation performed by a verifier on a correct transcript for the POW, as described in the specification at page 6. lines 17-20. Claim 28 clearly defines what is included and excluded in the claim, and is not an omnibus claim.

Withdrawal of the rejection of claim 28 under 35 USC 112, second paragraph is requested.

Paragraph 8:

A. Claim 25 has been amended to define the term "w" before its use and provide an antecedent for the term "V". The amendment of claim 25 overcomes the rejection under 35 USC 112, second paragraph.

B. Claim 26 has been amended to delete the variables (w, p, m) before their definition. Withdrawal of the rejection of claim 26 under 35 USC 112, second paragraph is requested

C. Claim 27 has been amended to define a variable (w) before its use. The amendment of claim 26 overcomes the rejection under 35 USC 112, second paragraph. Withdrawal of the rejection of claim 27 under 35 USC 112, second paragraph is requested. 1

Paragraph 9:

The period mark after the term "and" has been deleted. Withdrawal of the objection to claim 25 is requested.

Paragraph 10:

Claims 1-7, 12-15, 17 and 23-28 include features not disclosed in Rose and overcomes the rejection under 35 USC 102 (e), as follows:

A. Claim 1:

For reasons previously discussed above, Rose fails to disclose the claimed subject

matter, as follows:

1. There is no distributed computational task being accomplished.

2. Rose fails to disclose an entity demonstrating a certain amount of computation has been performed by a user within a specified interval of time.

3. Rose fails to disclose a first entity receiving a response compiled from more than two entities

4. Rose fails to disclose recycling a puzzle of a user to another user.

B. Claims 2-4 further define claim 1 and are patentable on the same basis as

claim 1.

C. Claims 5-7 describe claim 1 in a minting operation. Applicants can find no disclosure in Rose relating to minting coins as described in Jakobsson in Figure 3. In any case, Claims 5-7 are patentable on the same as claim 1-4.

D. Claims 12-15 further describe a minting operation and are patentable on the same basis as claims 5-7.

E. Claim 17 further describes claim 13 and is patentable on the same basis as claim 13.

F. Claim 23 further defines claim 13 and is patentable on the same basis as claim 13.

G. Claims 24-28 further define claim 1 and is patentable on the same basis as claim 1.

Summarizing, the rejection of claims 1-7; 12-14, 17 and 23-28 under 35 USC 102 (e) is not supported in Rose, which fails to disclose (a) a distributed computational task performed by a plurality of entities, (b) an entity demonstrating a certain amount of computation has been performed within a specified time interval, (c) a POW compiled from computations performed by a plurality of entities, and (d) recycling of a POW. Withdrawal of the rejection and allowance of claims 1-7, 12-5, 17 and 23-28 are requested.

Paragraph 11:

Claim 8, 9 and 11 include limitations not disclosed or suggested in Rose in view of Van Hook, of record, and overcome the rejection under 35 USC 103 (a), as follows:

A. Claims 8 & 9:

"The method of claim 6 wherein said predetermined image comprises a range of images. and wherein all images within said range of images have a predetermined number of least significant bits in common."

Van Hook does not supply the missing elements in Rose relative to predetermined images comprising a range of images having a predetermined number of least significant bits in common. Van Hook appears to use hash functions of a different type than is used in cryptography. There are two types of computation known as hashing. The one that Van Hook relates to is not collision resistant, and is not hard to invert. The Jakobsson hash functions are collision resistant and hard to invert. Van Hook cannot practice his invention with a cryptographic hash function. To do so, would render his technique meaningless. Whereas Jakobsson could distribute any type of hashing Function. Moreover, finding partial hash collisions is not meaningful in the context of hash functions of the type disclosed by Van Hook.

In particular, Van Hook, at col. 9, lines 55-67, discloses hashing an index of coordinate values descriptive of an image where the hashed index value is used to map the memory locations in main memory. The locations are referred to by (s) "and (t) coordinates". The hashed index enables coordinates varying in only a few bits to be mapped to different locations in a cache memory. In contrast, Applicants, at pg. 11, lines 8-12, disclose an entity transmits a hash function to be used in identifying collisions within a predefined search space for pre-images that have a range of images whose "t" least significant bits have the value "s". Van Hook hashes an index of coordinates for an image location and fails to disclose hashing the coordinates of a range of images that map to a single image.

Van Hook, at col. 11, line 13-25, discloses a process for cache index hashing for an (s) coordinate that is fed into first and second portions on a (t) address is fed into first and second portions. The division of coordinates can be based on some number that most or least significant bits or any other suitable scheme. The cited text does not disclose or suggest images within a range of images have a predetermined number of least significant bits in common.

Summarizing, applicants describe a linking operation that identifies valid solutions that hash to a range of images for a predetermined image. Van Hook does the opposite of Jakobsson by reducing the likelihood that adjacent addresses will match the map to the same cache region. Moreover, the Examiner has not demonstrated in any respect a motivation or reasonable expectation of success in combining Van Hook with Geer to implement a computational effort invested in a proof of work for accomplishing a minting operation. Finally, Geer and Van Hook fail to disclose all of the limitations of claim 8 and 9.

The rejection of claims 8 and 9, under 35 USC 103(a) is not supported in the cited art. Withdrawal of the rejection and allowance of claims 8 and 9 are requested.

B. Claim 11:

Claim 11 further limits claims 5 and 6 in overcoming the rejection under 35 USC 103 (a), and is patentable on the same basis as claim 5.

Paragraph 12:

Claims 10 and 18 include limitations not disclosed or suggested in Rose, in view of Xaio, of record, and overcome the rejection under 35 USC 103 (a) as follows:

Xiao does not supply the missing limitations in Rose. Xiao, at col. 2, lines 26-53 discloses the parameters for real-world scheduling/sequencing to accommodate different conditions and able to adapt to changes. Applicants can find no disclosure in Xiao relating to searching a different solution search space for valid solutions, as described in the specification at pg. 11, line 20 continuing to pg. 12, line 5. The scheduling/sequencing problems and evolutionary computation used in resolving those manufacturing scheduling problems, does not disclose or suggest sub-task searching different solution search space for valid solutions. Without such disclosure, there is no basis for a worker skilled in the art to implement claims 10 and 18. The rejection of claims 10 and 18 under 35 USC 103(a) fails for lack of support in the prior art. Withdrawal of the rejection and allowance of claims 10 and 18 are requested.

The motivation to modify Rose by the teachings of Xiao to produce a near optimal or optimal sequence of products for manufacture does not enable a worker skilled in

the art to implement a minting operation in a computational effort invested in a POW. The rejection of claims 10 and 19, based on 35 USC 103(a) is without support in the cited art. Withdrawal of the rejection and allowance of claims 10 and 18 are requested.

Paragraph 13

Claims 16 and 19-21 include features not disclosed or suggested in Rose in view of Simon, of record and overcome the rejection under 35 USC 103 (a), as follows

Simon fails to disclose the missing limitations in Rose. Simon, at col. 8, lines 65 to col. 9, line 15, discloses public keying encryption and the use of message authentication codes to ensure that messages between parties are not tampered with by someone other than the sender. Applicants can find no disclosure in Simon relating to using a suitable hash function and string concatenation, including a secret value, for generating a coin to be minted, as described in the specification at pg. 13, lines 3-14.

A worker skilled in the art would not be motivated to modify Rose with Simon to implement a method of accomplishing a minting operation using a computational effort invested in a POW. Without such motivation or reasonable expectation of success, and the failure of the cited references to describe all of the claim limitations, there is no basis under 35 USC 103(a) for the rejection of claim 16 and 19-21.

Withdrawal of the rejection and allowance of claims 16 and 19-21 requested.

Paragraph 14:

Claim 22 includes limitations not disclosed in Rose, in view of Puhl, of record, and overcomes the rejection under 35 USC 103 (a), as follows:

"The method of claim 19 wherein said hash is of a concatenation of a solution and a value generated using said secret value."

Puhl fails to disclose the missing limitation in Rose. Puhl, at col. 17, lines 24-42, discloses storing secret keys and member certificates in a wireless identity module software token. The member keys are protected by pass phrase information. The information is

concatenated with a secret value for the device and run through a secure hash in order to generate encryption/encryption key for use in protecting the user's private key. In contrast, applicants at page 13, lines disclose a hash function is concatenated with a secret value "r" specific to each coin to be minted. The computation performed aids in the successful completion of the task of finding the requisite number of pre-image values that hash to a specific range of images for the purpose of minting coins. Puhl discloses hashing for generating encryption/encryption keys and not for the purpose of minting coins.

A worker skilled in the art would not be motivated to modify a method of modeling an enterprise, via a wireless electronic commerce system, to implement a minting operation having privacy using a hash operation and a secret value. Further, the Examiner has not demonstrated any reasonable expectation of success for such a combination to implement the method of claim 22. The rejection of claim 22 is without support in the cited art. Withdrawal of the rejection and allowance of claim 22 are requested.

CONCLUSION

Applicants have established the cited art does not disclose or suggest a computational task distributed among a plurality of entities for generation of a Proof of Work (POW) which is recyclable. Accordingly, the rejection of claims 1, 2, 4-6, 8-28 under 35 USC 102(e) or 35 USC 103(a) is without support in the cited art. The application is in condition for allowance. Entry of the amendment, allowance of the claims, and passage to issue of the case are requested or alternatively, entry of the amendment for purposes of appeal is requested.

AUTHORIZATION:

The Commissioner is hereby authorized to charge any additional fees which may be required for consideration of this Amendment to Deposit Account No. 13-4503, Order No. JAKOBSSON 23-5 (3037-4196). A DUPLICATE OF THIS DOCUMENT IS ATTACHED.

In the event that an extension of time is required, or which may be required in addition to that requested in a petition for an extension of time, the Commissioner is requested to grant a petition for that extension of time which is required to make this response timely and is hereby authorized to charge any fee for such an extension of time or credit any overpayment for an extension of time to Deposit Account No. 13-4503, Order No. JAKOBSSON 23-5 (3037-4196). A DUPLICATE OF THIS DOCUMENT IS ATTACHED.

Respectfully submitted,
MORGAN & FINNEGAN, L.L.P.

Dated: May 26, 2006 By: Joseph C Redmond Jr

Joseph C. Redmond, Jr., Reg. No. 18,753
Telephone: (202) 857-7887
Facsimile: (202) 857-7929

CORRESPONDENCE ADDRESS:
Morgan & Finnegan L.L.P.
3 World Financial Center
New York New York